Política de Segurança

Safety Software | Aktualizacja: 03.09.2026 | https://safetysoftware.eu

<?xml encoding="utf-8" ?>

Política de Segurança da Aplicação Safety Software (SaaS)

ID: SE-2026-V2
Atualização: 2026-03-05

1. Objetivo e âmbito

A presente Política de Segurança define os princípios de proteção das informações e dos dados tratados no âmbito da aplicação Safety Software disponibilizada no modelo Software as a Service (SaaS).

O documento diz respeito à segurança dos utilizadores que usam a aplicação no serviço Safety Software e constitui um complemento aos Termos e Condições e à Política de Privacidade.

A Política tem caráter informativo e descreve as medidas técnicas e organizacionais básicas aplicadas pela Safety Software Sp. z o.o., ul. Półłanki 80, 30-740 Cracóvia, Polónia (doravante: “Administrador”).

2. Modelo de responsabilidade

O sistema funciona num modelo de responsabilidade partilhada:

1. **Administrador (Safety Software)** é responsável pela segurança do código da aplicação, mecanismos de login, autorização e sessão, proteção de dados na camada aplicacional, realização de cópias de segurança e resposta a incidentes de segurança.

2. **Fornecedores de infraestrutura e serviços auxiliares** são responsáveis pela segurança dos elementos que permanecem no âmbito dos serviços por eles prestados.

3. **Cliente** é responsável pela segurança dos seus dispositivos, palavras-passe, identidades dos utilizadores e pela gestão dos acessos na sua equipa.

3. Princípios de segurança da aplicação

1. A transmissão de dados ocorre exclusivamente com utilização de cifragem TLS.

2. As sessões dos utilizadores são protegidas com cookies com os atributos **HttpOnly**, **Secure** (para ligações cifradas) e **SameSite**. Após a autenticação, ocorre a rotação do identificador de sessão.

3. Para as sessões são aplicados limites de inatividade e de duração máxima.

4. Pedidos que alteram o estado do sistema são protegidos por tokens CSRF verificados no lado do servidor.

5. A aplicação aplica uma política de segurança de conteúdo restritiva, incluindo mecanismos que limitam a execução de scripts não autorizados e cabeçalhos de segurança padrão do navegador.

6. São aplicados mecanismos que limitam abusos, incluindo rate limiting e proteção contra tentativas de login por força bruta.

7. Cada operação é executada no contexto do utilizador e da organização; o acesso não autorizado é bloqueado.

4. Cifragem e proteção de dados

1. As palavras-passe dos utilizadores são armazenadas com utilização do algoritmo **bcrypt**.

2. Determinados dados sensíveis armazenados na base de dados são protegidos através de um modelo de cifragem de dados por envelope. As chaves criptográficas são geridas separadamente num sistema externo de gestão de chaves.

3. Quando justificado, são aplicados mecanismos que limitam a exposição de dados, preservando as funções de pesquisa ou identificação, sem necessidade de armazenar valores completos em texto claro.

5. Backup e recuperação (BCP/DR)

1. Aplicamos uma abordagem em camadas às cópias de segurança: cópias locais para recuperação rápida e cópias armazenadas fora do ambiente principal.

2. As cópias armazenadas fora do ambiente principal incluem imagens do ambiente executadas de forma incremental. Estas são cifradas, validadas regularmente e abrangidas por testes de recuperação.

3. A base de dados é protegida por cópias consistentes a nível da aplicação. Adicionalmente, são mantidos dumps locais da base de dados que suportam uma recuperação rápida.

4. A integridade das cópias é verificada através de mecanismos de controlo, incluindo somas de verificação.

5. O processo de execução de cópias é automatizado, realizado diariamente e sujeito a monitorização do sucesso e do insucesso das tarefas.

6. São realizados regularmente testes de recuperação de dados, incluindo pelo menos a recuperação de ficheiros selecionados.

6. Monitorização e alertas

1. O sistema regista determinados eventos de segurança e operações administrativas, em particular os relacionados com a autenticação, tentativas de acesso e o funcionamento de processos críticos.

2. São aplicados mecanismos de monitorização e alertas automáticos sobre falhas de tarefas, erros críticos e eventos que possam indicar abuso ou um incidente de segurança.

3. O acesso a logs e a informações operacionais é limitado a pessoas autorizadas.

7. Infraestrutura e manutenção da segurança

1. O acesso administrativo é limitado a pessoas autorizadas e protegido por

mecanismos de autenticação forte, incluindo autenticação por chaves.

2. O login direto numa conta privilegiada é desativado ou limitado de acordo com o princípio do menor privilégio.

3. São aplicados mecanismos de filtragem de tráfego, proteção contra tentativas de acesso por força bruta e monitorização de eventos de infraestrutura.

4. As atualizações de segurança são implementadas regularmente.

5. Os serviços de correio eletrónico utilizados para suporte do sistema são protegidos por cifragem da transmissão e por mecanismos que limitam abusos.

8. Fornecedores e integrações

1. Na medida em que o sistema utiliza serviços externos ou integrações auxiliares, a seleção de soluções tem em conta a segurança dos dados, o princípio da minimização e o controlo do âmbito das informações transmitidas.

2. A comunicação com serviços externos ocorre com utilização de transmissão cifrada.

9. Comunicação de incidentes

As comunicações relativas à segurança da aplicação ou suspeitas de incidentes devem ser dirigidas para o endereço:

office@safetysoftware.eu
Assunto da mensagem: SECURITY

As comunicações são analisadas de acordo com o procedimento interno de tratamento de incidentes.

10. Conformidade e jurisdição

1. As medidas de segurança são concebidas e mantidas tendo em conta as disposições legais aplicáveis, incluindo os requisitos do **RGPD**, e as práticas reconhecidas de segurança da informação.

2. A lei aplicável é a lei polaca.

3. Em caso de divergências entre versões linguísticas, prevalece a versão polaca.

11. Entrada em vigor

A presente versão da Política de Segurança é válida a partir de **2026-03-05**.

A versão atual do documento é publicada no serviço Safety Software.

Administrador de dados e proprietário do sistema:
Safety Software Sp. z o.o.
ul. Półłanki 80
30-740 Kraków, Polónia
E-mail: **office@safetysoftware.eu**

Registo de alterações

Atualização: 2026-03-05

- precisaram-se as cópias de segurança em camadas e o processo de restauro de dados (BCP/DR)
- completou-se a descrição da cifragem de dados com o modelo de envelope e a gestão externa de chaves
- alargou-se a descrição da proteção aplicacional com sessões, CSRF, CSP e mecanismos antiabuso
- adicionou-se a secção de monitorização e alertas e simplificou-se a secção de integração com serviços externos